NOTICE: When government or other drawings, specifications or other data are used for any purpose other than in connection with a definitely related government procurement operation, the U. S. Government thereby incurs no responsibility, nor any obligation whatsoever; and the fact that the Government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use or sell any patented invention that may in any way be related thereto.

FTD-TT- 63-248

6332

TRANSLATION

AN OPTIMUM IDENTIFYING DEVICE FOR SYSTEMATIC CODES AND CERTAIN TYPES OF CHANNELS

BY

I. I. Grushko

FOREIGN TECHNOLOGY DIVISION

AIR FORCE SYSTEMS COMMAND

WRIGHT-PATTERSON AIR FORCE BASE
OHIO

UNEDITED ROUGH DRAFT TRANSLATION

AN OPTIMUM IDENTIFYING DEVICE FOR SYSTEMATIC CODES AND CERTAIN TYPES OF CHANNELS

By: I. I. Grushko

English Pages: 9

SOURCE: Russian Periodical, Izvestiya Akademii Nauk SSSR, OTN, Energetika i Avtomatika, Nr 3, 1961, pp 105-109

S/24-61-0-3-7/12

THIS TRANSLATION IS A RENDITION OF THE ORIGINAL FOREIGN TEXT WITHOUT ANY ANALYTICAL OR EDITORIAL COMMENT. STATEMENTS OR THEORIES ADVOCATED OR IMPLIED ARE THOSE OF THE SOURCE AND DO NOT NECESSARILY REFLECT THE POSITION OR OPINION OF THE FOREIGN TECHNOLOGY DIVISION.	PREPARED BY: TRANSLATION SERVICES BRANCH FOREIGN TECHNOLOGY DIVISION WP-AFB, OHIO.

Date 20 March 1963

AN OPTIMUM IDENTIFYING DEVICE FOR SYSTEMATIC CODES AND CERTAIN TYPES OF CHANNELS

I. I. Grushko

A method of constructing an optimum identifying device for systematic correcting codes is considered. In this case it is assumed that the channel is given at the output of the threshold device by the stochastic matrix of the conversion of the elementary signals.

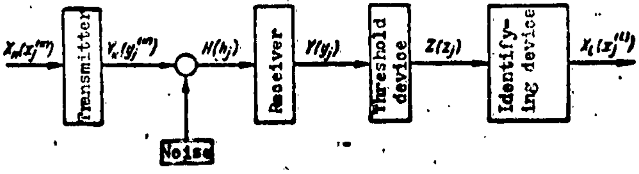
A number of authors have suggested transmitting messages through discrete communication channels with the aid of uniform n-valued correcting codes with the base γ and m information positions. In this case the following sequence of symbols enters the transmitter input (see figure)

$$X_k = (x_1^{(k)},\ldots, x_j^{(k)},\ldots, x_n^{(k)}) \qquad (k = 1,2,\ldots, \gamma^m) \tag{1}$$

The transmitter converts X_k into a complex signal Y_k, which is a set of elementary signals (not necessarily time-separated)

$$Y_k = (y_1^{(k)},\ldots, y_j^{(k)},\ldots, y_n^{(k)}), \tag{2}$$

where the elementary signal $y_j^{(k)}$ corresponds to the symbol $x^{(k)}$. It is assumed that the elementary signals are distinguished by one parameter (amplitude, phase, etc.).



As a result of the action of the channel noise on the signal (2), the following random signal will be obtained at the receiver input

$$H = (h_1, \ldots, h_j, \ldots, h_n \tag{3}$$

where h_j is a distorted elementary signal $y_j^{(k)}$. From the random signal (3) the following signal will be formed at the receiver output

$$Y = (y_1, \ldots, y_j, \ldots, y_n) \tag{4}$$

Here y_j is a random value of the parameter $\underline{y}$ of the signal h_j. The receiver is followed by a threshold device, in which the assumed value of the parameter $\underline{y}$ is identified with one of the possible values. At the output of the threshold device the result of the action of the noise on the elementary signals is represented in the form of the stochastic matrix of the transformation of the symbols

$$\| p_{ij} \| \tag{5}$$

where p_{ij} is the probability that in transmitting the i-th symbol it will be received as the j-th at the output of the threshold device. Henceforth we shall regard this matrix as given. We shall also assume that the nose distorts the elementary signals independently. At the output of the threshold device we obtain a certain code combination

$$Z = (z_1, \ldots, z_j, \ldots, z_n)$$

which, generally speaking, does not coincide with any one of the possibly transmitted ones. Therefore, the threshold device is followed by an identifying device, which identifies the obtained code combination Z with one of the possibly transmitted ones X_l according to some indicator or other. The most widespread indicator used in the existing literature is the minimum distance (in the sense of Hemming) between the code combinations Z and X_l. Obviously, in choosing an appropriate indicator it is necessary to proceed from a certain criterion and type of stochastic matrix (5).

Let us take as the basic criterion the maximum probability of correct reception of the code combination, and let us consider how to construct an identifying device in the best possible way for the chosen code (i.e., a certain fixed set of γ^m code combinations out of all the possible γ^n) and for the given channel (i.e., the given matrix $\|p_{ij}\|$).

Let us impose one more restriction: we shall assume the given code to be systematic. This means that the code combinations can be written in the form

$$X_k = (x_1^{(k)},\ldots,x_m^{(k)},x_{m+1}^{(k)},\ldots,x_n^{(k)}) \quad (k = 1,2,\ldots,\gamma^m)$$
$$x_i^{(k)} = l_i(x_1^{(k)},\ldots,x_m^{(k)}), \quad i = m+1, \quad m+2,\ldots,n \qquad (1')$$

where $l_i(x_1^{(\kappa)},\ldots, x_m^{(\kappa)})$ are certain linear functions which determine the correcting positions of the code combination in terms of information positions. Moreover, the functions $l_i(x_1^{(\kappa)},\ldots, x_m^{(\kappa)})$ have the following conditions imposed on them:

1) Each separate correcting position is formed according to completely determined rules, which are always the same for a given code combination;

2) The numbers of the positions being verified do not depend on a set of information symbols, i.e., on which of the numbers 0, 1, ..., γ - 1 occupy the information positions of the given code combination.

The restriction imposed has no essential significance, since it follows from the literature [1, 2] that systematic codes behave with respect to noise immunity and speed of transmission of information in approximately the same way as nonsystematic codes. On the other hand, this restriction has a number of advantages:

1) For systematic codes there exists a well developed apparatus of elementary group theory;

2) All the code combinations behave identically during transmission;

3) The coding is accomplished fairly simply;

4) In certain cases there are no better codes;

5) For certain types of channels it is possible to construct an optimum identifying device that is simple and lends itself to practical realization.

Let us consider how to construct an identifying device for the chosen code and the given channel in the best possible way with respect to the assumed criterion of maximum probability of correct reception of a code combination.

Let the channel be described by the stochastic matrix $\| p_{ij} \|$ of the transformation of the elementary signals. Since, by assumption, the channel noise distorts the individual positions of the code combination independently, the probability of a conversion of the code combination $X = (x_1, \ldots, x_n)$ into the code combination $Y = (y_1, \ldots, y_n)$ at the output of the threshold will be written in the form

$$P(X \to Y) = \prod_{i=1}^{n} p_{x_i y_i} \tag{6}$$

Let us assume that

$$P(X \to Y) = \frac{1}{f(X, Y)}$$

where $f(X, Y)$ is a function of X and Y satisfying the condition

$$f(X, Y) = f(X + Z, Y + Z) \tag{7}$$

for any X, Y, and Z.

Let a systematic code A, determined by formula (1), be given (note that among the elements of the code there always exists a zero element, i.e., a code combination $X_0 = (0, 0, \ldots, 0)$*. Let us choose a certain element Y_1, which does not belong to set A, and construct a set A_1 of all code code combinations of the type

$$Y_1 + X_1$$

where $X_i (i = 1, 2, \ldots, \gamma^m)$ runs through all the elements of code A. Then let us choose an element Y_2, which belongs neither to A nor A_1, and construct a set A_2 of all code combinations of the type

$$Y_2 + X_i, \ X_i \epsilon A$$

And so on until we exhaust the set of all possible n-valued code combinations with elements assuming one of the values: $0, 1 \ldots, \gamma - 1$. It can be shown [3] that the sets A, A_1, A_2 ... thus constructed have an equal number of elements and do not intersect, i.e., there does not exist a code combination such that it would belong simultaneously to more than one of the sets A, A_1, A_2, ... Let us write out the sets A, A_1, A_2, ... in rows in the form of a table:

Code A	X_0	X_1	X_2	...	X_μ
Set	Y_1	Y_1+X_1	Y_1+X_2	...	Y_1+X_μ
	Y_2	Y_2+X_1	Y_2+X_2	...	Y_2+X_μ
$A_k=(Y_k+X_i;\ X_i \in A)$	...	...	...	...	...
	Y_ν	$Y_\nu+X_1$	$Y_\nu+X_2$	...	$Y_\nu+X_\mu$

where $\mu = \gamma^m$ and $\nu = \gamma^{n-m}$.

* It can be readily demonstrated that any systematic code (1) is a subgroup in the additive group of all n-dimensional sequences over the ring of residue classes modulo γ with respect to the operation of coordinate-wise addition.

We shall call the table normal if

$$f(X_0,Y_k) \leqslant f(X_0, Y_k + X_i) \qquad (8)$$

From elementary group theory [3] it follows that any of the elements of the set A_j may be chosen as the generating element of A_j. Therefore, in constructing a normal table, it is sufficient to choose from each row of the table an element Y_k such that condition (8) is satisfied, after which an appropriate permutation is made.

In accordance with the literature [4], let us use the following scheme (Slepian's detector) for the identifying device: if an element Z, obtained at the output of the threshold device, is located in the i-th column of the normal table, the detector gives the code combination X_i at the receiving end.

The following theorem is valid:

Slepian's detector is a maximally reliable scheme of identification for a channel satisfying condition (7), i.e., for the given code A it gives the greatest probability of correct reception of a code combination.

Actually, the code combination being used occupies a certain definite position in the normal table, i.e., there exists a pair of subscripts k and j such that

$$Z = Y_k + X_j$$

Taking into account that the following formula is always valid for any code combination T

$$X_0 + T = T$$

we obtain from condition (7)

$$f(X_0, Y_k) = f(X_0 + X_j, Y_k + X_j) = f(X_j, Y_k + X_j)$$
$$f(X_0, Y_k + X_i) = f(X_0 + X_j, Y_k + X_i + X_j) = f(X_j, Y_k + X_l)$$

for any $j, l = 1, 2, \ldots, \mu$; $k = 1, 2, \ldots, \nu$. In this case the element $X_l = X_i + X_j$ runs through the entire code A for fixed i and any j = 1, 2, ..., μ. Substituting the result obtained in (8), we obtain

$$f(X_j, X_k + X_j) < f(X_j, Y_k + X_l)$$

for any j, l = 1, 2, ..., μ; k = 1, 2, ..., ν. By virtue of the condition

$$P(X \to Y) = \frac{1}{f(X, Y)}$$

This means that Slepian's detector ensures the greatest probability of correct reception of a code combination for a given code and channel.

Let us consider certain examples.

1. In most of the literature on coding (Slepian's, in particular [4]) a so-called binary symmetrical channel is analyzed. Let us consider a symmetrical channel with any number of elementary signals γ. This channel is described by the stochastic matrix $\| p_{ij} \|$

$$\begin{gathered} p_{ii} = q, \\ p_{ij} = p_{i+1,\, j} = p_{i,\, j+1} = p \quad (i \neq j) \end{gathered} \tag{9}$$

for all i, j = 0, 1, ..., γ - 1.

By virtue of conditions (9) the value of (6) in the given case depends only on the number of positions in which the code combination X differs from the code combination Y, i.e., the probability of a conversion of the code combination X into the code combination Y is a function of the Hemming distance ρ(X, Y) between the code combinations X and Y and is equal to

$$P(X \to Y) = p^{\rho(X,Y)} q^{n - \rho(X,Y)}$$

(the Hemming distance ρ(X, Y) between code combinations X and Y is determined as the number of positions in which X and Y differ from each other). By virtue of a coordinate-wise determination of the operation of addition of the code combinations, the Hemming distance ρ(X, Y) satisfies the condition

$$\rho(X, Y) = \rho(X + Z, Y + Z)$$

for any code combinations X, Y, and Z.

Therefore, choosing as the function f(X, Y) the quantity

$$f(X,Y) = p^{-\rho(X,Y)} q^{\rho(X,Y)-n}$$

we can construct an optimum identifying device. Since

$$\ln f(X, Y) = \rho(X, Y) \ln \frac{q}{p} - n \ln q$$

the inequality (8), by virtue of the continuity of a logarithmic function, leads to the inequality

$$\rho(X_0, Y_k) \leqslant \rho(X_0, Y_k' + X_i)$$

for all k = 1, 2, ..., ν and i = 1, 2, ..., μ. This means that in order to construct a normal table determining an optimum identifying device, the elements Y_j (j = 1, 2, ..., ν) must be chosen in such a way that within the space of the signal they are not located beyond (in the sense of Hemming distance) all the other elements of the set $A_j = \{Y_j + X_i;\ X_i \in A\}$. The result obtained agrees with Slepians [4] in the case of a binary symmetrical channel.

2. The stochastic matrix of the channel $\|p_{ij}\|$ has the form:

$$p_{ii} = q$$
$$p_{ij} = e^{-a(i-j)^2}, \quad i \neq j$$

for all i, j = 0, 1, ..., γ - 1. In this case the probability of a conversion of a code combination X into a code combination Y will be written in the form

$$p(X \to Y) = q^k e^{-ad^2(X,Y)} = q^{n-\rho(X,Y)} e^{-ad^2(X,Y)}$$

where k is the number of coinciding positions in the code combinations X and Y, while d(X, Y) is an ordinary distance in a Euclidean metric.

By virtue of a coordinate-wise determination of the addition of the code combinations, we have

$$d(X,Y)=d(X+Z,Y+Z), \quad \rho(X,Y)=\rho(X+Z,Y+Z)$$

Thus, choosing as f(x, y) the function

$$f(X,Y)=q^{\rho(x,y)-n}e^{\alpha d^{2}(x,y)}$$

we can construct an optimum identifying device in the way described above.

Received on January 31, 1961

REFERENCES

1. P. Elias. Coding for Two Channels with Interference. Symposium "Theory of Transmission of Messages", Foreign Language Publishing House , 1957.

2. R. L. Dobrushin. The Asymptotics of the Probabilities of Errors in Transmitting Information Through a Channel Without a Memory and with a Symmetrical Matrix of the Probabilities of Conversion. DAN SSSR, 1960, Vol. 33, No. 2.

3. A. G. Kurosh. Group Theory. Fizmatgiz, 1955.

4. D. Slepian. A Class of Binary Signal Alphabets. Symposium "Theory of Transmission of Messages", Foreign Language Publishing House, 1957.

DISTRIBUTION LIST

DEPARTMENT OF DEFENSE	Nr. Copies
HEADQUARTERS USAF	
AFCIN-3D2	1
ARL (ARB)	1
OTHER AGENCIES	
CIA	1
NSA	6
DIA	9
AID	2
OTS	2
AEC	2
PWS	1
NASA	1
ARMY (FSTC)	3
NAVY	3
NAFEC	1
RAND	1
PGE	12

MAJOR AIR COMMANDS	Nr. Copies
AFSC	
SCFDD	1
DDC	25
TDBTL	5
TDBDP	5
SSD (SSF)	2
APGC (PGF)	1
ESD (ESY)	1
RADC (RAY)	1
ASD (ASYIM)	1
AFSWC (SWF)	1
AFMTC (MTW)	1